ABSTRACT

An encryption and decryption system and method for message forwarding in a multi-node network which provides fast message forwarding while minimizing CPU time and power requirements by unconditional decryption of all incoming messages and unconditional encryption or re-encryption of all outgoing messages, which pass through a forwarding node or nodes. Messages from a source node to the destination node pass through the forwarding node, which unconditionally decrypts the incoming message from the source node without prior determination of the ultimate destination of the message. The forwarding node then unconditionally re-encrypts the outgoing or forwarded message for transmission to the destination node.